

# MULTIMEDIA NETWORK APPLIANCES FOR SECURITY AND SURVEILLANCE APPLICATIONS

INVENTOR: David A. Monroe

5

## BACKGROUND OF THE INVENTION

Field of the Invention. The subject invention is generally related to sensor, monitor and control appliance devices generally utilized in monitoring and surveillance systems and  
10 is specifically directed to a network adaptation of such appliances.

Discussion of the Prior Art. Security of public facilities such as schools, banks, airports, arenas and the like is a topic of increasing concern in recent years. Over the past few years, a number of violent incidents including bombings, shootings, arson, and hostage situations have occurred. In addition, agencies responsible for public security in these facilities must cope with more commonplace crimes, such as drug dealing, vandalism, theft and the like.

Such facilities frequently employ monitoring and surveillance systems and access control systems to enhance security. This has been common practice for a number of years. Such systems generally have a centralized monitoring console, usually attended by a guard or dispatcher. A variety of sensors are located throughout the facility, such as smoke detectors, fire detectors, motion sensors, glass breakage detectors, badge readers at various access points, and sometimes, video cameras and/or microphones. Other sensors and transducers are utilized to lock and unlock doors.

There are numerous devices utilized to collect information at remote locations and  
25 initiate a local alarm, store the information for later retrieval or forward the information to a remote location for storage and/or near real time review. Examples include fire alarms, security cameras, motion sensors, proximity switches, heat sensors, smoke and fire sensors, and the like. Almost all of these appliances can be used in some form of configuration where one or more sensors may be used in combination to provide a surveillance scheme over an  
30 area to be monitored. In prior art systems, the signal generated by each type of device was used locally, or if part of a network, was sent over a dedicated connection to a remote collection point for that type of device.

TELETYPE

These prior-art devices often use technologies that not ‘intelligent’ in the modern sense; they merely provide an ‘ON/OFF’ indication to the centralized monitoring system. The appliances also are not ‘networked’ in the modern sense; they are generally hard-wired to the centralized monitoring system via a ‘current loop’ or similar arrangement, and do not provide situational data other than their ON/OFF status.

5

## SUMMARY OF THE INVENTION

The subject invention is directed to support function systems that may be used separately or in combination as building support devices by adapting them to network appliances and configuring them to communicate over network topologies to each other, to building databases, and to the users. This allows either stand alone functional systems, or a fully integrating them into a single “seamless” system. By way of example, school classrooms may have several communications and monitoring systems to support a classroom such as an intercom, clock system, thermostat, motion detector, door access control, computer network connections and the like. The subject invention permits the combination of all of these functions into a single device that may communicate over a single network connection providing various combinations to provide for building support functions. The devices may also communicate to other buildings and control nodes in other facilities by use of Wide Area Networks (WANs) such as Intranets and the Internet.

The invention is particularly well adapted for use in connection with my co-pending patent applications, entitled: Multimedia Surveillance and Monitoring System Including Network Configuration, Serial No. 09/594,041, filed on June 14, 2000; Method and Apparatus for Distributing Digitized Streaming Video Over a Network, Serial No. 09/716,141, filed on November 17, 2000; and Method and Apparatus for Collecting, Sending, Archiving and Retrieving Motion Video and Still Images and Notification of Detected Events, Serial No. 09/853,274, filed May 11, 2001, and incorporated by reference herein.

The subject invention includes specific network appliances designed to participate in a comprehensive multimedia security and building support system that may be deployed singularly or in combination to achieve the degree of monitoring and protection desired.

10  
15  
20

25

5       The subject invention also permits all of the support functions to be combined in one appliance, achieving both improved functionality and support at a lower costs because of use of shared components, shared wiring and shared network connectivity. In the preferred embodiment, the appliance is connected to a single Category5 (CAT5) wire, fiber or the like to the system network. The single appliance provides all of the functions previously supplied by a plurality of dedicated purpose discrete appliances.

10      Functional superiority over the discrete appliances is also achieved because of the opportunity to integrate the various subsystems common in the appliances. For example, a universal wall appliance in accordance with the subject invention can use a common display panel for a clock/bell system and a visual alarm. A single microphone can be shared for the intercom, for noise detection and for alarm oral response or activation. A single speaker can be utilized for the intercom, a telephone call bell, an alarm emitter and a clock/bell sound emitter. A single temperature sensor can be shared between a fire alarm system, the HVAC system and be utilized to check for appliances proper ambient operating temperature environment. A wireless LAN access point can be shared for remote or mobile alarm/sensor/display modules and for classroom computer access. A single video camera can be shared for security monitoring, video conferencing and distance learning. A single streaming audio/video decoder can present Video On Demand (VOD) classroom video presentations, broadcast television and video conferencing.

20      The subject invention permits network components and appliances to be used in combination with a network based full service, multi-media surveillance system capable of a wide range of monitoring techniques utilizing digital network architecture.

25      Schools, banks, retail operations and other security conscious businesses and institutions have a need for advanced hardware and software solutions that provide total, user friendly control over their surveillance and monitoring equipment. A system desirably provides:

1.     Multimedia data collection;
2.     Automated control;
3.     Archive storage;
4.     Enhanced search and recall of archived event recordings;

5. Preset responses to triggers and triggering events;
6. Remote viewing and management from a wide area network including, preferably, the World Wide Web (or Internet) accessibility.
7. Automatic system pre-failure prediction and post failure analysis.
8. Common infrastructure and workstations shared with other co-located systems.
9. Wireless infrastructure for sensors, monitors and shared applications/systems.

In accordance with the teachings of the subject invention, any or a plurality of distinctive appliances may be connected to the comprehensive, wired/wireless multimedia surveillance and monitoring system for transmitting event data, video and/or image monitoring information, audio signals and other network appliance sensor and detector data over significant distances using digital data transmission over networks such as a local area network (LAN), a wireless LAN (WLAN), a wide area network (WAN) such as the Internet for other network automatic event recording, assessment and response, including dispatch of response personnel. Wired, wireless and optical appliances and sensor systems may be employed. The wireless LAN connectivity permits local distribution of sensor, audio, video and image data with relatively high bandwidth without expensive local wiring/fiber and without the requirement of a license and without relying on a common carrier and the fees associated therewith. The surveillance system may be interfaced with a WAN (wide area network) such as optical fiber, frame relay or the Internet for providing a worldwide, low cost surveillance system with virtually unlimited geographic application. Centralized and distributed remote monitoring stations have access to all of the surveillance data from various remote locations via the network or the WAN. A server provides a centralized location for data collection, alarm detection and processing, access control, auto response generation, paging, automatic e-mail generation, telephone dialing and message transmission, dispatch processing, logging functions, configuration management, and/or other specialized functions. The server may be inserted virtually anywhere in the Intranet/Internet network, and may be segmented and installed in a distributed manner to further add to system security, reduce bandwidth requirements, or allow redundancy.

5

10

15

20

25

30

35

40

45

50

55

60

65

70

75

80

85

90

95

Multiple sensors and appliances may be accommodated, as required. The topology of the network will be established by the geographic situation of the specific installation. Appropriate firewalls, encryption and access codes may be set up as desired to protect unauthorized access to the system or collected data. The server based system permits a security provider to have access to the appliance, related sensor and surveillance data or to configure or reconfigure the system from any station on the Intranet or Internet.

The system of the subject invention permits comprehensive monitoring of locations over great distances with sufficient performance to provide widespread use as a security surveillance device.

The subject invention is specifically directed to networked appliances such as video and/or image appliances, access control devices, detectors and sensors as well as audio, condition and/or event monitoring systems. In its preferred form, the comprehensive multi-media safety and surveillance system of the subject invention provides both visual and audio information as well as critical data such as temperature fire and smoke detection. Manually operated transducers, such as panic buttons, door contacts, floor sensors, and the like may also be included to activate the system in the presence of an event at the sensor location, such as a fire alarm or security alarm panic bar or the like. Controlled transducers, such as electric door strikes, magnetic door strikes, electric door openers, strobe lights, sirens, room lights, fire control equipment and the like can be controlled by the appliances. Numerous appliances, including but not limited to detection and sensor systems, are utilized to provide monitoring stations or personnel, such as security personnel, and/or a base station monitoring critical information from the sensor system and to record the information and permit reconstruction of events after the fact.

In its preferred form, a plurality of sensor units, which may include at least one video image appliance sensor and/or at least one audio appliance sensor and/or at least one motion appliance sensor and/or other sensors, are placed strategically about the facility to be monitored. In addition, strategically placed motion detectors, fire sensors, panic switches, smoke sensors and other monitoring equipment is incorporated in the system. Cameras may be placed throughout the facility and in other desired spaces including on the grounds outside

5

10

00000000000000000000000000000000

20

25

the facility. The audio sensors/transducers and other sensors and detectors are also strategically located both internal and external of the facility.

While the appliances of the subject system may be hardwired, in its preferred form the system of the present invention is adapted for use in connection with wireless transmission and receiving systems. The wireless system is particularly useful for adapting the system as a retrofit in existing facilities and also provides assurances against disruption of data transmission such as during a fire, as well as permitting roving interactive monitors that can be carried or worn. In the preferred embodiment, the wireless system is fully self-contained with each appliance and/or sensor unit having an independent power supply and, where required for image sensors, a sensor light source. The security system may include either motion sensitive, audio sensitive and/or image processing based activation systems so that the equipment is not activated until some event is detected, i.e., the system is action triggered.

In the preferred embodiment, each appliance will transmit any detected information to a monitor system located at a base monitoring station, located on site and/or at a remote or roving location, and/or a server for logging, forwarding, archiving same. The base station has instant live access to all of the image and audio signals as they are captured by the sensors, and where desired is adapted to record and make an historic record of the images for archive purposes. Where random access recording techniques are used, such as, by way of example, digital random access memory storage devices or high speed disk storage arrays, the archive may be readily searched for stored information.

One significant advantage to the appliance configuration of the subject invention is that it permits multimedia surveillance in applications and locations where physical wiring cannot be used, and over distances not possible or not cost effective with other systems. The system of the present invention provides surveillance capability utilizing techniques ranging from closed-circuit, hard wired systems to the Internet based techniques and is not limited by the data capacity; or cost associated with systems currently on the market.

It is, therefore, an object and feature of the subject invention to provide both wired and wireless communication links between appliances, sensors, monitors and/or sensors.

5 It is an additional object and feature of the subject invention to provide an appliance configuration for a multimedia surveillance system adapted for any of a plurality of monitoring and surveillance appliances which may be incorporated in the system via network connections through a server to provide a versatile, wide-ranging multi-media system which may be configured to meet specific application needs.

It is an additional object and feature of the subject invention to provide an appliance and monitoring station configuration for a multimedia surveillance system adapted for a plurality simultaneously operating geographically distributed monitoring stations.

10 It is another object and feature of the subject invention to provide appliances adapted for use in connection with a surveillance system for transmitting data over significant distances using typical bandwidth carriers such as the public telephone system, and wireless carriers such as cellular telephones, including AMPS, PCS, GSM, CDMA, wide band CDMA and the like, CDPD data links, two-way pagers, satellite networks such as Iridium and the like.

15 It is another object and feature of the subject invention to provide appliances adapted for use in connection with a surveillance system for transmitting data over significant distances using typical broadband carriers such as cable TV networks, dedicated fiber optics networks, DSL and ADSL carriers, and forthcoming broadband wireless networks.

20 It is also an object and feature of the subject invention to provide appliances for a surveillance system adapted for utilizing wired video and/or image data collection and/or transmission using the Internet and/or IP protocols.

25 It is also an object and feature of the subject invention to provide appliances for a surveillance system adapted for utilizing wireless video and/or image data collection and/or transmission using the Internet and/or IP protocols.

It is also an object and feature of the subject invention to utilize network communication systems to distribute both appliance surveillance data and control data.

30 It is another object and feature of the subject invention to provide network appliances for a security surveillance system adapted for use in connection with a wireless LAN (WLAN) communications system, such as the IEEE 802.11 standards and follow-on standards.

It is another object and feature of the subject invention to provide time display to a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide emergency event annunciation to a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide room paging through a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide room audio monitoring utilizing a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide room intercom utilizing a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide room temperature sensing using a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide device temperature sensing using a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide room gunshot detection utilizing a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide room access control utilizing a network appliance communicating over the IP network.

It is another object and feature of the subject invention to provide an audio monitor or intercom between one or more network appliances and one or more monitor system using voice-over-IP (VOIP).

It is another object and feature of the subject invention to provide an audio monitor or intercom between two or more network appliances utilizing VOIP.

It is another object and feature of the subject invention to provide archival storage of VOIP audio information for later playback.

It is another object and feature of the subject invention to provide a network appliance with video and/or audio capability with muted camera video and/or muted microphone audio capability in a room for privacy.

It is another object and feature of the subject invention to provide a network appliance device that has an open camera and/or microphone when panic button is pushed.

It is another object and feature of the subject invention to provide “intercom” and “emergency” buttons on a panic button.

It is another object and feature of the subject invention to provide panic button initiated actions, such as:

- 5           Intercom functions to and from room over IP.
- Logging of all intercom calls.
- Emergency notification to wired guard stations over IP.
- Emergency notification to wireless guard stations over IP.
- Push-To-Talk (or voice activation) response from guard or administrator.
- 10          Display on room display stating identity of the responding party.
- Flashing location icon on map for intercom or emergency.
- Pop-up name of person pushing panic button.
- Pop-up location of person pushing panic button.
- Pop-up name of room where emergency is taking place.
- Logging of all panic button pushes, by whom, time, location, and the like.
- Logging of all responses, by whom, time, and the like.
- Recording of all emergency audio/video on server or appliance.
- For emergency calls, automatic call list: i.e., if first guard does not respond, go to next, go to administration.
- 20          For emergency calls, have a party line: i.e., call all stations, all can respond asynchronously.
- On party line, all stations display the name of any speaker doing a push-to-talk (or voice activation) operation, with workstations having a pop-up display and wall appliance display shows instead of time.
- 25          A software priority is established for the responding push to talk (or voice activation). Automatic notification priority based upon location, nearest, first, and so on.
- It is another object and feature of the subject invention to provide a workstation-to-workstation intercom utilizing VOIP.

It is another object and feature of the subject invention to provide push-to-talk or voice activated control of audio from two or more stations on a group session at one time.

It is another object and feature of the subject invention to provide an audio/video intercom from workstation-to-workstation utilizing VOIP.

5 It is another object and feature of the subject invention to provide map-based dialing to workstations or network appliances.

It is another object and feature of the subject invention to provide menu-based dialing to workstations or network appliances.

It is another object and feature of the subject invention to provide IP video to and from network appliances.

It is another object and feature of the subject invention to provide logging of all calls.

It is another object and feature of the subject invention to provide logging of all calls with caller and/or called station ID's.

It is another object and feature of the subject invention to provide logging of all calls with time stamps for time of calling and answering.

It is another object and feature of the subject invention to provide logging of all calls by recording actual audio on the server.

It is another object and feature of the subject invention to provide calls to guard stations and standard PC workstations.

It is another object and feature of the subject invention to provide calls to administrative stations.

It is another object and feature of the subject invention to provide calls from any workstation to any other workstation.

It is another object and feature of the subject invention to provide other voice interfaces, such as:

Calls patched into POTS telephone calls from the “outside” through a gateway network appliance device.

Calls on internal PBX through a gateway network appliance device.

Multimedia network appliances can be patched into VOIP telephone calls such as from the Internet, VOIP phone systems and the like. Incoming calls are automatically distributed.

Outgoing calls by automatic priority, such as guard station first, if no answer, the police department over POTS.

Outgoing calls by speed dialing. It is another object and feature of the subject invention to provide access control, such as:

Access granted or denied flashing on map.

Automatic camera switching based on any access attempt.

Automatic camera switching on access denied only.

Mode for manual guard confirmation for all accesses.

Access network appliance powered over Cat-5 wiring.

Access network appliance controlled over IP wiring.

Access control of a network appliance decided by server, or by internal tables.

Access network appliance has internal access allowance tables set over IP wiring.

Access network appliance uses internal tables if server is down.

Access network appliance always uses internal tables (to save bandwidth).

Access network appliance has encryption.

Access network appliance has contact outputs.

Access network appliance has optional wireless badge reader.

Access network appliance has optional swipe badge reader.

Access network appliance has optional fingerprint reader.

Access network appliance has optional retina scanner.

Access network appliance has link to personal geo-locator such that if authorized person is in close proximity door opens.

Access network appliance opens under local control.

Access network appliance opens under server control.

Access network appliance has tamper detectors reporting over IP.

Access network appliance sends all activity to server for logging.

Access network appliance has local memory for logging all activity.

Access network appliance can send local memory content to server for logging.

Server can request access network appliance data for logging.

Access network appliance is configured over IP.

Access network appliance has HTML server for setup and monitoring.

5 Access network appliance supports friendly names, such as “East Outside Door”.

Access network appliance has password protection.

Access network appliance has encrypted communications to and/or from.

Access network appliance can communicate over wired LAN (example, cat-5).

10

Access network appliance can communicate over wireless LAN (example IEEE 802.11B).

Other objects and features will be readily apparent from the accompanying drawings and detailed description.

#### **BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 is a perspective view of a room network appliance module in accordance with the subject invention.

Fig. 2 depicts an overall block-diagram view of a simple implementation of a wall network appliance of the type shown in Fig. 1.

Fig. 3 illustrates a network-supported circuit for communicating a time standard to a network appliance for use in event logging or event execution by a network appliance via a local network.

Fig. 4 shows a configuration including a network hub embedded into the security network appliance.

Fig. 5 shows a configuration wherein a room network appliance includes wireless networking technologies.

25

Fig. 6 illustrates the utility of the room network appliance as configured as an integrated multimedia sensor for a plurality safety-related sensors commonly employed in such a facility.

Fig. 6A is a wireless version of network appliance shown in Fig. 6.

30

Fig. 7 depicts a room network appliance as a gathering point for room environmental data.

Fig. 7A is a wireless version of the network appliance shown in Fig. 7.

Fig. 8 illustrates a network appliance enhancement including a video camera, digitizer, motion video compressor, still-frame video compressor, infrared illuminator for dark operation, audio sensor, digitizer, and audio compressor.

5

Fig. 8A is a wireless version of the network appliance shown in Fig. 8.

Fig. 9 illustrates a room network appliance with an alternative alarm source wherein a wireless “panic button” alarm device may activate the system.

10

Fig. 9A is a wireless version of the room network appliance shown in Fig. 9.

Fig. 10 illustrates one method power insertion technique utilizing the LAN data link incorporated in the system of the invention to power a wired network appliance.

20

Fig. 11 depicts an alternative embodiment including an alternate power insertion technique whereby DC power conveyed along signal pairs of the cable, in common-mode, in order to power a wired network appliance.

Fig. 12 depicts a motion detector sensor network appliance with an IP network interface and power receiver.

Fig. 12A is a wireless version of the network appliance shown in Fig. 12.

Fig. 13 depicts a networked smoke detector network appliance using the network interface of Fig. 12.

Fig. 13A is a wireless version of the network appliance shown in Fig. 13.

Fig. 14 depicts a conventional ‘Pull Handle’ commonly used in institutional fire alarm systems as adapted for incorporation in the networked appliance of the subject invention.

25

Fig. 14A is a wireless version of the network appliance shown in Fig. 14.

Fig. 15 depicts a contact-closure interface, as is commonly used for door or window sensors in alarm systems as adapted as a networked appliance of the subject invention.

Fig. 15A is a wireless version of the network appliance shown in Fig. 15.

Fig. 16 depicts a heat sensor network appliance.

Fig. 16 A is a wireless version of the network appliance shown in Fig. 16.

Fig. 17 depicts a glass breakage sensor network appliance.

30

Fig. 17A is a wireless version of the network appliance shown in Fig. 17.

Fig. 18 depicts an alarm siren network appliance.

Fig. 18A is a wireless version of the network appliance shown in Fig. 18.

Fig. 19 depicts a strobe light network appliance.

Fig. 19A is a wireless version of the network appliance shown in Fig. 19.

5

Fig. 20 depicts a thermostat/humidistat network appliance.

Fig. 20A is a wireless version of the network appliance shown in Fig. 20A.

Fig. 21 depicts a general-purpose control panel network appliance.

Fig. 21A is a wireless version of the network appliance shown in Fig. 21.

Fig. 22 depicts a simple control switch network appliance.

10

Fig. 22A is a wireless version of the network appliance shown in Fig. 22.

Fig. 23 depicts an indicator light panel network appliance.

Fig. 23A is a wireless version of the network appliance shown in Fig. 23.

Fig. 24 depicts a networked analog user interface control network appliance, such as may be used to control room lights, temperature, fan speed, louver blind position, loudspeaker volume, and the like.

Fig. 24A is a wireless version of the network appliance shown in Fig. 24.

Fig. 25 depicts a loudspeaker network appliance.

Fig. 25A is a wireless version of the network appliance shown in Fig. 25.

Fig. 26 depicts a control panel network appliance with indicator lights.

20

Fig. 26A is a wireless version of the network appliance shown in Fig. 26.

Fig. 27 depicts a power outlet network appliance.

Fig. 27A is a wireless version of the network appliance shown in Fig. 27.

Fig. 28 illustrates an AC socket as expanded into a network-controlled AC power strip network appliance.

25

Fig. 28A is a wireless version of the network appliance shown in Fig. 28.

Fig. 29 depicts a telephone interface/dialer network appliance.

Fig. 29A is a wireless version of the network appliance shown in Fig. 29.

Fig. 30 depicts a lighting fixture network appliance controlled over a network.

Fig. 30A is a wireless version of the network appliance shown in Fig. 30.

Fig. 31 depicts an analog wall clock network appliance controlled over the IP network.

Fig. 31A is a wireless version of the network appliance shown in Fig. 31.

Fig. 32 depicts an alternative embodiment of the network appliance of figure 31, wherein a digital display replaces the stepper motor, gearbox, hands and shaft encoder.

Fig. 32A is a wireless version of the network appliance shown in Fig. 32.

Fig. 33 depicts a self-contained magnetic strip reader network appliance, containing a reader as is commonly used in ATM machines, gas pumps, and point-of-sale cash registers.

Fig. 33A is a wireless version of the network shown in Fig. 33.

Fig. 34 depicts a proximity card reader network appliance.

Fig. 34A is a wireless version of the network appliance shown in Fig. 34.

Fig. 35 depicts an electronic door strike controller network appliance shown controlling a standard electo-mechanical door strike.

Fig. 35A is a wireless version of the network appliance shown in Fig. 35.

Fig. 35 B is a self-contained electronic door strike network appliance with an integrated IP network interface and electro-mechanical door strike.

Fig. 35 C is a wireless version of the network appliance shown in Fig. 35 B.

Fig. 36 depicts a combination security controller network appliance showing as it is utilized to control an electronic door strike, a door contact switch, a keypad entry system, and a secondary identification component such as a magnetic stripe reader, a proximity sensor or retina reader, or the like.

Fig. 36A is a wireless version of the network appliance shown in a Fig. 36.

Fig. 37 depicts a combination security controller network appliance controlling an electric door strike, and sensing door contacts and a proximity sensor Fig. 37A is a wireless version of the network appliance shown in Fig.37.

Fig. 37 B is an electronic strike network appliance with external contact inputs.

Fig. 37 C is a wireless version of the network appliance shown in Fig. 37B.

Fig. 38 depicts a combination network appliance that is controlling an electric door strike and sensing door contacts and a magnetic stripe reader. Fig. 38 A is a wireless version of the network appliance show in Fig. 38.

Fig. 39 depicts a keypad entry network appliance with auxiliary electric strike and door contacts.

Fig. 39 A is a wireless version of the network appliance shown in Fig. 39.

Fig. 40 shows a wireless proximity sensor network appliance.

5 Fig. 39A depicts the circuit diagram for the system of Fig. 39

Fig. 39B depicts the circuit diagram for a wireless version of the system of Fig. 39.

Fig. 40 shows a system similar to the system shown in Fig. 39 with the addition of an exit sign.

Fig. 40A depicts the circuit diagram for the system of Fig. 40.

10 Fig. 41 depicts a wired universal interface-pull handle/strobe system.

Fig. 41A is a wireless version of the system shown in Fig. 41.

Fig. 42 depicts a wired pull handle system.

Fig. 42A is a wireless version of the system shown in Fig. 42.

Fig. 43 depicts a wired exit device.

Fig. 43A is a wireless version of the system shown in Fig. 43.

Fig. 44 depicts a wired keypad mortise lock.

Fig. 44A is a wireless version of the system shown in Fig. 44.

Fig. 45 depicts a wired magnetic card stripe swipe reader mortise lock.

Fig. 45A is a wireless version of the system of Fig. 45.

Fig. 46 depicts a wired proximity card reader mortise lock.

Fig. 46A is a wireless version of the system of Fig. 46.

Fig. 47 is a control center system and diagram for connecting various sensors to the system.

Fig. 47A is a wireless version of the system of Fig. 47.

25 Figs. 48 and 49 depict multiple universal interface applications.

Fig. 50 is a block diagram of the multiple appliance security system in accordance with the invention.

Figs 51 and 51A-\* comprise a full schematic of the system in accordance with the block diagram of Fig. 50.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 depicts an overall view of the appliance 5 of the subject invention. The appliance contains a variety of devices that are commonplace or useful in educational, institutional, or office environments, including:

- 5 • A conventional clock display 25, operable to display other information as needed such as temperature, humidity, alert messages, etc.
- 10 • A microphone 35, to detect local ambient sounds in the room and send them to a remote location and, optionally, to support acoustic event detection of gunshots and the like,
- A loudspeaker 20, to allow remote supervisory personnel to communicate with room occupants,
- A beacon transmitter 30, which emits coded infrared, RF, or ultrasonic energy into the room for the purpose of activating personnel locator devices therein,
- A beacon receiver also 30, which detects coded infrared, RF, or ultrasonic energy emitted by locator devices within the room,
- A camera 15, to view live or still scenes in the room and send them to a remote location,
- A standard RJ-45 or equivalent connector 40 for connecting to a facility Network.
- An antenna 10 may be provided for supporting a wireless connection, as will be explained therein.

Fig. 2 depicts an overall block-diagram view of a simple implementation, such as may be used in an educational setting. In this implementation, the appliance only supports a clock display 65, a loudspeaker 45, and a microphone 55, to support the ordinary clock and intercom commonly found in schoolrooms. As shown, a digital-to-analog converter 50 and an analog-to-digital converter 60 are used as required for conditioning signals input to and output from the signal processor 70. The system processor is connected to a network interface 80, and/or as desired a wireless interface 85. The wireless interface 85 is in wireless communication with a wireless access point 87 for providing a gateway to the network 90.

5

10

20

20

25

30

The device is connected to a local-area-network, such as the commonplace 10Base-T, via the network interface. 10Base-T networks commonly employ twisted-pair wiring between hubs and connected devices; an alternative implementation may use IEEE 802.11 or equivalent wireless connections. In either case, the network interface passes information to and from the appliance's processor. The processor controls the clock display. Ambient sounds picked up by the microphone are digitized, compressed, and transmitted to the network via the A/D converter, signal processor, system processor, and network interface. A variety of compression methods and communication protocols may be employed; in the preferred embodiment the audio is compressed using MP3 and sent to the network using the RTP and TCP/IP protocols. Similarly, compressed audio from the network may be received, de-multiplexed, decoded, and played back via the network interface, system processor, signal processor, and D/A converter.

As depicted in Fig. 3, the clock may be set from a time server 110 connected to the local network 115. A variety of network-based time-transfer methods exist, the most popular and convenient is Network Time Protocol (NTP), a protocol used in conjunction with local-area networks or the Internet. Using NTP, the time server and the client (in this case, the appliance) exchange time messages, and determine a statistical value for network delay, which is then factored out. Accuracies on the order of 1 millisecond are possible on a local network. The timeserver may be set manually, or may optionally be set using a commercially available WWV time receiver 100 or GPS time receiver 105. As an alternative, the local time server may set itself to an internet-based master timeserver, such as provided by NIST or the U.S. Naval Observatory (USNO) as indicated by the network timeserver 125, via the network 120. Various security appliances including the security circuits 94 may be incorporated in the circuit via the network interface 95.

A useful refinement of the system is depicted in Fig. 4. As there shown, the appliance processor 130 is connected to an embedded network hub 140 via a network interface 135. Typically, a 10Base-T hub, or equivalent, is embedded into the appliance. This allows other computers 150, 155, printers 145, or other networked devices (via network 160) to share the existing connection from the room to the facility's local area network. By

way of an example, remote workstation 157 may be supported in this manner. An archival server 161 is accessible over the network 160.

The local area network hub may also include wireless networking technologies, such as the IEEE 802.11, as depicted in Fig. 5. In this enhancement a wireless LAN access point 180 and an antenna 175 is provided at the appliance, permitting communication with various wireless remote components or systems such as the printer 195 supported by the wireless adapter 205 and antenna 200, the wireless desktop PC 215 and antenna 210, the wireless laptop 225 or other portable device and antenna 220.

Fig. 6 illustrates the utility of the room appliance as a collection point for safety-related sensors such as, by way of example, the microwave motion detector 230, the infrared motion detector 235, the smoke detector 240, and the carbon monoxide detector 250, commonly employed in such a facility. The processor 265 collects data from the various sensors in the room. Such inputs are often simple contact closure inputs. When activated, the appliance alerts a security monitoring station via the local network or via a wide-area network 275 through the network interface 270. The security station may then summon the appropriate help, such as police, fire, ambulance, or other services as needed. Also, the system processor when so activated may generate an appropriate local warning sound using the D/A converter 260 and the loudspeaker 255. Appropriate sounds might be a fire horn, alarm bell, klaxon, or the like. The warning sounds may be generated from stored sounds in the processor's memory, or may be generated by the facility security system and transmitted to the room appliance via the intervening network. As shown, various remote stations such as a logging server or archive server 161, a security monitoring station 280 and other systems such as by way of example the environmental monitoring controller 281.

Fig. 6A is a wireless version of the system of Fig. 6. In this enhancement a wireless interface 283 is provided for communicating with a wireless access point 287 to provide a link to the network 275. Also in this embodiment a power supply 289 and a converter 291 is provided to power the appliance system. In the wired version the network cabling is used to provide power.

Fig. 7 depicts the room appliance as a gathering point for room environmental data, as may be used in controlling an HVAC system. Various environmental control sensors, such

5

10

1234567890

20

25

30

as a relative humidity sensor 285, temperature sensor 290, or thermostat panel 295, may connect to the facility HVAC controller 315 via the room appliance processor 265 and network 310. Other critical monitoring systems such as, by way of example, the fire alarm controller 316, may be interconnected to this subsystem via the network. The wireless version is shown in Fig. 7A.

Fig. 8 illustrates an enhancement to the basic appliance system, wherein a video camera 325, digitizer 330, motion video buffer 335 and compressor 340 and, optionally, a still-frame video buffer 345 and compressor 350 is added. An illuminator 320 for low light conditions may also be supplied. When activated, the camera captures local scenes, and transmits them to a monitoring station(s) 390 on the local network or wide-area network using suitable compression methods such as MPEG or JPEG, via the network comprising the multiplexer 355, the system or appliance processor 375 and a network interface 380 whereby communication via the network 385 is supported. Simultaneously, the microphone 360 may be included to receive local sounds, digitize them at converter 365, compress them at compressor 370, and send them to the same destinations. Activation of the camera and microphone may be accomplished locally via one or more of the attached sensors, or remotely via the network from a monitoring station. If the ambient illumination is insufficient for viewing via the camera, an illuminator may be enabled by command from the appliance's processor or by command from the remote station. The illuminator may be visible light or infrared, as desired. A wireless version is shown in Fig. 8A with an independent power supply 289, converter 291 and wireless access point 287 is provided as previously described.

An alternative alarm source is depicted in Fig. 9, wherein a wireless "panic button" alarm device 440 may activate the system using the wireless transmitter 445 and receiver 450, 455. As shown, the wireless alarm has an RF receiver 455 and transmitter 465, controlled by the T/R switch 460, a device ID memory 475, and a pushbutton switch 480. A process controller 470 is also provided. During normal usage, the room appliance 485 periodically transmits a code representing its location. The personal alarm 440 receives and stores this location code. When the alarm is activated by pressing the switch 480, the alarm transmits its device ID and the room ID information to the appliance 440. This then activates

the appliance, enabling the camera and microphone, and alerts the central monitoring station via the intervening network. As shown, the appliance 440 in this configuration includes a compatible RF receiver 400, T/R switch 405, RF transmitter 410 with antenna 395. The appliance processor 425 and network interface 430 communicate with the network 435 as previously described. An encoder 420 may be provided as necessary. Fig. 9A shows the same system with wireless network interfacing as previously described.

Figs. 10 and 11 depict a standardized method and apparatus for monitoring, controlling, and powering a variety of network-based appliances, which are subsequently described. This is advantageous when the network-based may be located in an area where conventional AC-operated power is not easily accessible. Referring to Fig. 10, a conventional LAN data link is depicted. The hub's physical-layer interface 800 connects to twisted-pairs 815 and 820 via transformers 805 and 810. The remote network device's physical-layer interface 830 connects to the same twisted pairs 815 and 820 via transformers 825 and 830, thus effectuating a conventional LAN connection. Twisted-pair cable typically used in LAN's generally contains 4 pairs, who of which are unused in this example. Accordingly, one or both of the unused twisted-pairs 855 and 865 are employed to convey operating power to the remote device. A power source 840 is disposed at the centralized hub or switch. The power source is preferably a voltage source, and preferably a DC source of moderately high voltage. Typical voltage levels may run in the 30 to 60 Volt range. Current sensor 845 senses the DC current consumed by the remote device, and may cause current limiter 850 to reduce or eliminate any current supplied to the remote device, in the case of a fault in the wiring or in the remote device. At the remote device, power is extracted and regulated by regulator 860, preferably a switched-mode down-converter of high efficiency.

Fig. 11 depicts a variation of the same method, wherein the DC power is conveyed along the signal pairs of the cable 855, 865, in common-mode. In this example, transformers 805, 810, 825, and 830 are center-tapped, and the power is applied to the center taps of transformers 805 and 810. Said power is extracted from the center taps of transformers 825 and 830 at the remote device. As before, power is supplied by source 840, and is monitored and protected by current sensor 845 and limiter 850. At the remote end, power extracted from the center taps of transformers 825 and 830 is appropriately regulated by regulator 860.

The network interface, common to all subsequent network devices, here represented as the motion sensor 525, is depicted in Fig. 12. The device attaches to the network using RJ-45 connector 520. An Ethernet interface 515 handles the physical-layer connection to the Ethernet network. The required DC operating power, as supplied over the network wiring, passed through RJ-45 connector 520 to the Ethernet Line-Power Interface 510. This interface extracts the DC power provided by the network, and provides filtering and regulation as necessary to provide the DC operating voltages required by the device via line 505. The power provided by the network will typically be at a relatively high DC voltage for the sake of transmission efficiency. The Line-Power interface will therefore typically contain one or more regulators to reduce the line-supplied DC voltage to an appropriate value such as the standard 3.3 VDC or 5 VDC. An IP controller 500 is provided.

An additional benefit of the described configuration is that all sensors or appliances are intelligent due to the presence of the preprogrammed IP controller. This allows a centralized system monitoring station to automatically detect and configure the individual sensors or appliances. For example, a device may ‘announce’ itself immediately upon installation, thus becoming automatically recognized and monitored by the centralized monitoring station. Also, relevant operating parameters of the device may be measured or controlled remotely. An example might be a glass breakage detector with a history of false alarms; the sensor’s sensitivity may be reduced from the centralized monitoring station via the network. Fig. 12A shows a wireless version of the system depicted in Fig. 12. In this enhancement a wireless interface card 526 and receiver/transmitter 528 is provided at the device, for defining the wireless interface 380 that operates as previously described.

Figs. 13 through 34A depict a variety of additional sensors and appliances that may be attached to the described network. All these described devices share a common network interface, allowing any such device to be added to the network as desired. Moreover, all such devices are configured to derive their operating DC power from the network, rather than from locally supplied power.

Fig. 13 depicts a networked smoke detector, using the same standardized network interface of Fig. 12. The device may also contain a heat sensor, to increase the accuracy of detecting a fire. The smoke and heat sensors 530 and 535 pass their data to the IP controller

5

10

15

20

25

30

500, which generates and transmits a predefined message to the network. Note that the heat sensor may pass an actual numerical value for temperature to the network if desired, rather than a simple 1-bit indication that a temperature threshold has been exceeded. Fig. 13A is the wireless version and corresponds to the circuit shown in Fig. 12A.

Fig. 14 depicts a conventional ‘Pull Handle’ commonly used in institutional fire alarm systems. In this case, the input to the IP controller 500 is a simple 1-bit input from the pull handle switch 540. Again, the device sends a predefined IP message to the network and system monitoring station upon activation. Fig. 14 is the wireless version.

Fig. 15 depicts a simple contact-closure interface, as is commonly used for door or window sensors in alarm systems. The sensors often contain a magnet in one module, and a magnetic reed switch in the other module. In this implementation, the contact closure thus effectuated by the reed switch 545 becomes input bit into the IP controller 500. In response to a change in switch status, the controller 500 generates and transmits a predefined IP message via the Ethernet interface to the network and associated monitoring apparatus. Fig. 15A is the wireless version.

Fig. 16 depicts a networked heat sensor. The sensor 550 may produce a simple one-bit ‘threshold crossed’ indication to the controller 500, or may pass a variable representing actual sensed temperature. In either case, the IP controller 500 generates and transmits a predefined IP message to the network and associated monitoring apparatus. As an additional refinement, the device may be programmed to accept configuration commands from the networked monitoring apparatus. Such commands may, for example, change the sensor’s trip point or temporarily suspend the transmission of messages. Fig. 16A is the wireless version.

A networked glass breakage sensor is depicted in Fig. 17. Sensor 555 produces an output indicative of breaking glass to the IP controller 500, which generates a predefined IP message and transmits said message to the network. The sensor's output may, if necessary be processed or analyzed by controller 500 in the case of a simple microphone or vibration sensor. The device may additionally be configured to respond to incoming control and configuration messages from the network, such as commands to change the sensor's sensitivity or to temporarily disable the device. Fig. 17 is the wireless version.

5 Figs. 18 and 19 depict a networked alarm siren and strobe light respectively. The IP controller 500 receives IP messages from the network and controls the alarm 560 or strobe light 565 respectively. Network messages may be used to turn the alarm or strobe on or off, or may control other characteristics of the device such as volume, flash rate, etc. The IP controller may also send status messages to the network, either in response to inquiries from control devices or at regular intervals. Figs. 18A and 19A are the wireless versions, respectively.

10 Fig. 20 depicts a networked thermostat or humidistat, or both combined. The temperature sensor 570 and/or humidity sensor 575 produce signals indicative of local temperature and/or humidity. As before, IP controller 500 generates and transmits predefined messages to the network representing the current values of temperature and/or humidity. In addition, switches 580 and 585 allow a user to increase or decrease the desired temperature setting. Contact closures produced by switches 580 or 585 are detected by IP controller 500 and transmitted via IP messages to a monitoring and/or control device disposed on the network. In addition, display 590 displays the current value of the local temperature and/or temperature setting. The temperature displayed may be generated locally by the controller 500 or may be commanded by a networked monitoring and control device via IP messaging. Fig. 20A is the wireless version of the thermostat/humidistat network appliance.

15 A general-purpose control panel network appliance is depicted in Fig. 21. This is a highly flexible device that can be used for several multimedia monitoring functions, as well as many control functions. For example, the control network appliance can be utilized as a conventional type control keypad for alarm system functions. It also could be utilized for lighting control, HVAC control, pump control, fan control, volume control, and other facility management founctions. A keypad 595 and display 600 are connected to the IP controller 500. The controller 500 detects and interprets keystrokes on keypad 595, and generates appropriate IP messages for transmission over the intervening network to a networked monitoring and control station. Similarly, a networked monitoring and control station may 20 generate messages to be displayed on the control panel's display 600. Said messages are

transmitted from the monitoring and control station via the IP network to the controller 500, which causes the appropriate message to be displayed. Speaker 601 is provided for audible indications of keypad depression, status, alarms and for streaming of audio streams.

Fig. 21A is the wireless version of the control panel network appliance.

Fig. 22 depicts a simple control switch network appliance. The switch 605 may be a toggle, rocker, or push-button switch as appropriate. The status of switch 605 is detected by IP controller 500, which generates and transmits an appropriate message over the IP network to a networked monitoring and control station. The appliance may be configured to generate “on” and “off” signals for controlling a two state device, or with a center return momentary switch, can generate streams of “up” and “down” signal steams relating to the length of time that the button is held for “analog” controlling of devices.

Fig. 22A is the wireless version of the control switch network appliance.

An indicator light network appliance is depicted in Fig. 23. IP controller 500 receives messages from a networked monitoring and control station, and thereupon causes the appropriate lamp or lamps in light array 610 to be illuminated or extinguished. Fig. 23A is the wireless version of the indicator light network appliance.

Fig. 24 depicts an analog control device network appliance, such as may be used to control room lights, temperature, loudspeaker volume, fan speed and the like. IP controller 500 receives input from potentiometer 615 or shaft encoder 620, and thereupon generates appropriate IP messages and transmits them via the intervening IP network to a networked monitoring and control station.

Fig. 24A is the wireless analog control device network appliance..

A networked loudspeaker appliance is depicted in Fig. 25. In the preferred embodiment, the device receives a stream of data representing audio from the IP network. IP controller 500 passes this data to processor 625, which decodes the data stream and generates an appropriate analog signal for reproduction via loudspeaker 630. Control signals such as speaker amplifier gain, tone controls and the like can be sent to the loudspeaker appliance via the network.

Fig. 25A is the wireless version of the loudspeaker network appliance..

A control panel network appliance, with indicator lights is depicted in Fig. 26. Switches 635 and 640 cause the IP controller 500 to generate and transmit IP messages to a networked monitoring and control station. Additionally, a networked monitoring and control station may generate appropriate IP messages to control the status of lamps 645, 650, and 655 via the intervening network and IP controller 500. Fig. 26A is the wireless version of the control panel network appliance.

A networked power outlet is depicted in Fig. 27. In this device, the IP controller 500 controls the status of an AC power switch 670 in response to received IP messages from a networked monitoring and control station. The networked monitoring and control station may thereby turn an AC-powered appliance ON or OFF via networked IP messages. Alternatively, power switch 670 may be replaced with a dimmer module, to allow dimming of a lamp from the networked monitoring and control station. Additionally, an RJ-45 socket 665 may be installed on the device, to provide a local user with an Ethernet connection into the network. Effectively this allows the power control module to act as a network hub as well. Since the network connection to the network is already in use by the system controller 500, when another network connection port is needed such as 665, it is necessary to implement a simple three-port network hub 660 between the network physical-layer interface 515 and the RJ-45 connector to the network 520.

Fig. 27A is the wireless version. In the preferred embodiment the power for the network interface and control circuits are taken from the incoming AC power.

In Fig. 28, the network-controlled AC socket is expanded into a network-controlled AC power strip appliance. As previously described in Fig. 27, the IP controller 500 controls a switch or dimmer 670 in response to IP messages received via the network from a monitoring and control station. In this embodiment, multiple AC sockets 675 are provided. In addition, a circuit breaker 680 protects the device from overload. Surge protectors can also be implemented. Additional circuits can read the status of the power strip, such as the state of the circuit breaker, input voltage and the status of the surge protector. The current load of the power strip can also be measured. This allows for extensive “remote management” of the power strip over the network such as from a network operations center (NOC). Multiple power controllers, such as 670, can be implemented such as one for each

5 plug. This allows independent control of each plug. This could allow remote power cycling of a bank of network computers, for example, or would allow control of multiple temporary lighting circuits, stage lights, etc. Although the power strip network appliance can be powered by the incoming AC power line, if the power is not present the status of the strip could not be read. The network and control circuits can, however, be powered by the network connection as is described elsewhere in this application. This would allow the network devices to read the managed power strip status even if the incoming AC power is not available or the circuit breaker is tripped.

10 Fig. 28A is the wireless version of the power strip network appliance.

15 Fig. 29 depicts a network-controlled telephone dialer/interface, preferably housed in a standard telephone wall socket. A standard POTS telephone line or telephone is plugged into the telephone line 700 via RJ-11 socket 705. VOIP data can then be transferred from the phone line to the network, and from the network to the telephone line. If a central office (CO) line or private branch exchange (PBX) line is plugged into the RJ-11 jack, the RJ-11 interface is configured as a virtual telephone instrument. If a POTS telephone instrument is plugged into the RJ-11 socket, the RJ-11 interface is configured as a virtual telephone line. When configured as a virtual instrument, the IP controller 500, in response to commands received from the IP network, energizes relay 695, thus seizing telephone line 700. The IP controller 500 thereupon, in response to IP commands received via the IP network, causes DTMF generator 685 to produce the desired DTMF tones on telephone line 700 via line transformer 690. The interface also monitors the line to detect ringing and to detect caller-ID (CLID) data, and communicates that date via the LAN, then awaits for instruction to seize the telephone line. When configured as a virtual line, the network appliance supplies talk battery to the POT S telephone to power the telephone, the tone dial, and to detect off-hook conditions. It also generates a ring voltage to ring the POTS telephone when instructed to do so from instructions received over the network. This device has several uses in the multimedia system. It can be used to provide an interface to emergency telephones that are in communication with monitor stations. It is also used to interface to the telephone line for dialing and signaling under the control of the event notification services as is described in my other patents /patent applications. It also can be used a stand-alone relay for a voice circuit

between a pair if, or more, telephones, emulating an “order wire”. It also can be used as a bridge, providing a remote POTS telephone line via a LAN or WAN to another location for a POTS telephone instrument.

Fig. 29A is the wireless version of the telephone dialer/interface network appliance.

Fig. 30 depicts a lighting fixture network appliance controlled over the network. As in Fig. 27, IP controller 500 turns the light ON or OFF, or may dim the light, in response to IP messages received from a monitoring and control station via the network. The appliance can also monitor the status of the bulb and report over the network. This “managed bulb” can then be interrogated from a NOC, or a burned out bulb can generate an event that is notified to maintenance personnel for action by the notification services as described by my other patents/applications.

Fig. 30A is the wireless version of the lighting fixture network appliance.

Fig. 31 depicts an analog wall clock network appliance controlled by the IP network. IP controller 500 maintains an accurate knowledge of local time through periodic synchronization with a network time standard via SNTP or other appropriate network-time protocols. IP controller 500 drives a stepper motor 720, which drives hands 735, 740, and 745 via gear train 730. Shaft encoder 725 provides shaft position feedback information to IP controller 500, to allow the clock to be set after a power failure. The shaft encoder may be as simple as a one-bit indication that the hands are all in the 12:00 position.

Fig. 31A is the wireless version of the analog wall clock network appliance .

Fig. 32 depicts an alternative embodiment, the digital clock network appliance, wherein a digital display 735 and drive electronics replaces the stepper motor 720, gearbox 730, hands 735, 740, and 745, and shaft encoder 725. As before, IP controller 500 maintains accurate time via periodic synchronization over the IP network.

Fig. 32A is the wireless version digital clock network appliance.

Fig. 33 depicts a magnetic strip reader network appliance. The magnetic strip reader, as commonly used in ATM machines, gas pumps, and point-of-sale cash registers. Card reader 750 passes data extracted from the card to IP controller 500, which thereupon transmits the card data to a device on the IP network for appropriate processing. The card data is preferentially encrypted by IP controller before transmission, to provide security.

Fig. 33A is the wireless version magnetic strip reader network appliance.

Fig. 34 depicts a proximity card reader network appliance. This incorporates a proximity ID card readers, as commonly used at door entrances. IP controller 500 receives data detected by badge sensor 755, and passes an appropriate predefined IP message to a networked monitoring and control station.

Fig. 34 depicts a proximity card reader network appliance. This incorporates a proximity ID card readers, as commonly used at door entrances. IP controller 500 receives data detected by badge sensor 755, and passes an appropriate predefined IP message to a networked monitoring and control station.

Fig. 34A is the wireless proximity card reader network appliance.

It is an important feature of the subject invention that legacy sensors, alarms and devices may be connected to the multimedia network system without modification of the legacy devices, permitting signals generated by the legacy devices to be communicated via and managed by the system of the subject invention. Figs. 35-38 are examples of security network appliances that provide such enhancements. An important component of this feature is a common interface permitting the communication of the signals generated by the legacy device to the network supporting the system of the subject invention. One common interface network appliance device 900 is shown in Fig. 35 and includes two terminals or connectors 901,902 for connecting the output wires 904, 905 of a legacy device, here an electric door strike 906, to the network. The network connection is made via a wire connected at the RJ-45 jack 908.

As shown in Fig. 35A, the legacy device can also be connected via wireless interface 910. In this version, a power adapter 912 is provided for driving the interface 910. A wireless transmitter/receiver card 914 is added to provide the wireless network connection. In the wired version, the connector wire connected to the RJ-45 jack 908 is ideally used to provide power. However, a separate power supply can be provided where desired. Fig 35B shows an electric strike 906 with an RJ45 jack 908. Fig. 35C is the wireless version. Fig. 34 depicts a proximity card reader network appliance. This incorporates a proximity ID card readers, as commonly used at door entrances. IP controller 500 receives data detected by

badge sensor 755, and passes an appropriate predefined IP message to a networked monitoring and control station.

Fig. 34A is the wireless proximity card reader network appliance.

It is an important feature of the subject invention that legacy sensors, alarms and devices may be connected to the multimedia network system without modification of the legacy devices, permitting signals generated by the legacy devices to be communicated via and managed by the system of the subject invention. Figs. 35-38 are examples of security network appliances that provide such enhancements. An important component of this feature is a common interface permitting the communication of the signals generated by the legacy device to the network supporting the system of the subject invention. One common interface network appliance device 900 is shown in Fig. 35 and includes two terminals or connectors 901,902 for connecting the output wires 904, 905 of a legacy device, here an electric door strike 906, to the network. The network connection is made via a wire connected at the RJ-45 jack 908.

As shown in Fig. 35A, the legacy device can also be connected via wireless interface 910. In this version, a power adapter 912 is provided for driving the interface 910. A wireless transmitter/receiver card 914 is added to provide the wireless network connection. In the wired version, the connector wire connected to the RJ-45 jack 908 is ideally used to provide power. However, a separate power supply can be provided where desired. Fig. 35B shows an electric strike 906 with an RJ45 jack 908. Fig. 35C is the wireless version.

Multiple legacy appliances may be connected to a common interface network appliance system as shown in Fig. 36 (wired version) and Fig. 36A (wireless version). As there shown, the interface 920 has multiple terminals 901, 902, 920, 921 and 922 for contact type devices and/or appliance jacks 924, 925, such as could be in communication with RS-232 signals, for connecting numerous legacy appliances such as the retina reader 926, proximity reader 927, swipe reader 928 and keypad display 929. All of these are connected to the network via a connector such as a wire via RJ-45 jack 908 (Fig. 36) or via a wireless connection card 914 (Fig. 36A). As before, the power supply 912 may be used in either version.

Fig. 37 is an enhancement wherein a network sensor in accordance with the subject invention includes an integrated interface for connecting a legacy appliance to the network via the network sensor system. In this enhancement the proximity reader/controller 930 has an LED sensor 931 as is well known in the art and includes an RJ-45 jack for connecting the sensor to the network. As previously described, a wireless version is also supported. The sensor includes terminals or connectors 901, 902 and 920 for connecting various legacy appliances such as, by way of example the electric door strike 906 or the door contacts 923. Fig. 37A shows the wireless version. Fig. 37B shows a door strike 906 with an R45 jack 924 and optional door contacts 923. Fig. 37C is the wireless version.

Other sensors/devices may be similarly enhanced, as shown with the swipe reader 932 of Fig. 38.

38A is the wireless version of 38.

A keypad entry appliance 934 is similarly enhanced as shown in Fig. 39.

39A is the wireless version of 39.

A further enhancement is shown in Figs. 40-40C. In this enhancement a wireless proximity sensor 934 for monitoring movement within the marked zones, see zone 936, around monitored door 938 is connected to the network via the wireless transmitter/receiver card 526 and antenna 528 to a wireless access point interface 287. As is better shown in Fig. 40A, the circuitry for supporting this sensor 934 is identical to the circuitry shown and described in Fig. ???. The wireless version is shown in Fig. ??? and is consistent with the circuitry shown in Fig. ???A.

Figs. 40C and 40D show an enhancement of the door proximity sensor shown in Fig. ?? with a message display such as, by way of example, the EXIT display 940. In this configuration a power supply comprising the AC input, a transformer 942 and a battery charger 944 provides power to the display. This provides power to the lamp display 940 in the normal manner, and can also be used to power the IP controller 500.

The wireless connection can be made via a wireless antenna ~~943~~ or by coupling to the AC power wiring ~~945~~ such as through RF coupling capacitors ~~947~~. The wireless/power

carrier version is shown in Fig. 40D and is consistent with the changes made in the previously discussed embodiments.

Figs. 41 and 41A show a wired universal interface network appliance and wireless universal interface network interface, respectively. This configuration of the interface 946 includes an independent connection to a power supply as indicated at 948, or may be powered over the LAN 950 as has been previously discussed. The LAN connection such as the RJ-45 jack 950 in the configuration of Fig. 41 or the wireless connector 952 of Fig. 41A may be utilized. A plurality of terminal connectors 954 are provided for connecting the legacy devices such as the fire strobe display alarm 956 and the pull-handle alarm 958. The legacy devices can be powered from the LAN also, utilizing the power output terminals at 954.

Fig. 42 shows a pull-handle network appliance 959 modified for direct network hook-up using a wired RJ-45 jack 960. Fig. 42A is a wireless version of the pull-handle network appliance with the wireless modifications previously described.

A wired exit device network appliance is shown in Fig. 43. The wireless version of the exit device network appliance is shown in Fig. 43A. In this enhancement the exit device includes a latch 962, a push bar 964 and a key lock 966. Action on any of these elements will transmit a signal via wire 968 to show activity at the door. The wire is connected to terminals on the universal interface 946, which is in turn connected to the network 970 via a CAT-5 wire or other cabling to the universal interface. A wireless version is shown in Fig. 43A and includes the external power supply 289, the wireless access component 380, and the wireless access point 287, as with previously described enhancements.

A keypad mortise lock entry device network appliance is shown in Fig. 44, with the wireless version being depicted in Fig. 44A. The keypad lock device 972 includes a keypad 974, backup key lock 976 and a door handle 976, each of which will generate a signal when activated. The signal is carried from the control box 980 to a universal interface 946 for connection to the LAN 970. A wireless version is shown in Fig. 44A.

The keypad lock 974 is replaced by a card 986 and swipe reader 984 in Fig. 45 (wired) and Fig. 45A (wireless). A magnetic or optical card reader 990 and compatible card 992 is shown in Fig. 46 (wired) and Fig. 46A (wireless).

An alternative universal connector interface network appliance 996 is shown in Figs. 47 (wired) and 47A (wireless). The universal connector interface network appliance includes a plurality of terminals for providing power out (998), input from legacy devices (999) and various output signals other than network (1000). Applications of the universal interface network appliance are shown in Fig. 48 wherein an electric strike 1002 and latch 1004, an electric strike 1006 and a magnetic contact 1008. Fig. 49 shows additional universal interface applications using legacy appliances.

Fig. 50 is block diagram of the circuitry for supporting a multiple appliance security system in accordance with the subject invention. The full schematic is shown in Figs. 51 and 51A-51BB. With reference to Fig. 50, the security appliance 5 includes a system processor 75 having both Read Only Memory (ROM) and Random Access Memory (RAM) components 1025 and 1026, respectively. A contact closure interface 1028 is provided for connecting any combination of simple external appliances to the security appliance center. Specifically, these appliances are generally limited to ON/OFF conditions and responses. The RS-232 interface 1030 is provided for connecting more sophisticated external appliances such as, by way of example, the listed appliances and the appliances described elsewhere herein. A DTMF/CLID detector 1032 and phone line circuit monitor 1034 provides connection to an external telephone 1036 and to the telephone network 1038. External power is provided to the system either through the wired LAN interface 80 and the network power module 1040. External power may also be provided by the power supply 289 or through the option AC power brick 1042. The system is capable of wireless connection to the network 90 via the wireless network interface 85 and the wireless access point 87, or alternatively by wired connection to the network via network interface 80.

While certain embodiments and features of the invention have been described in detail herein, it will be readily understood that the invention includes all modifications and enhancements within the scope and spirit of the following claims.